Office of the Legislative Auditor

State of Montana

Report to the Legislature

June 1994

EDP Audit Report

Department of Labor and Industry

This report provides information regarding general and application controls over the Department of Labor and Industry's Unemployment Insurance Applications. It contains recommendations for improving controls over the department's electronic data processing environment. These recommendations address:

- Improving electronic access controls.
- Establishing formal contingency procedures.
- Improving report distribution procedures.

Direct comments/inquiries to:
Office of the Legislative Auditor
Room 135, State Capitol
PO Box 201705
Helena MT 59620-1705

94DP-41

EDP AUDITS

Electronic Data Processing (EDP) audits conducted by the Office of the Legislative Auditor are designed to assess controls in an EDP environment. EDP controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. In performing the audit work, the audit staff uses audit standards set forth by the United States General Accounting Office.

Members of the EDP audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business and public administration and computer science.

EDP audits are performed as stand-alone audits of EDP controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of four members of the Senate and four members of the House of Representatives.

MEMBERS OF THE LEGISLATIVE AUDIT COMMITTEE

Senator Greg Jergeson, Chairman	Representative John Cobb, Vice Chairman
Senator Gerry Devlin	Representative Ernest Bergsagel
Senator Eve Franklin	Representative Linda Nelson
Senator Tom Keating	Representative Robert Pavlovich

STATE OF MONTANA

Office of the Legislative Auditor

STATE CAPITOL
PO BOX 201705
HELENA, MONTANA 59620-1705
406/444-3122
FAX 406/444-3036

LEGISLATIVE AUDITOR:
SCOTT A. SEACAT

LEGAL COUNSEL:
JOHN W. NORTHEY

DEPUTY LEGISLATIVE AUDITORS:
MARY BRYSON
Operations and EDP Audit
JAMES GILLETT
Financial-Compliance Audit
JIM PELLEGRINI
Performance Audit

June 1994

The Legislative Audit Committee
of the Montana State Legislature:

This report is our Electronic Data Processing (EDP) audit of internal controls relating to the department's Unemployment Insurance (UI) applications. We reviewed the department's general controls as they relate to the UI applications. In addition, we reviewed application controls over the UI Tax and UI Benefits systems. This report contains recommendations for improving EDP controls at the department. Our recommendations include improving electronic access security, establishing formal contingency procedures, and improving report distribution procedures. Written responses to our audit recommendations are included in the back of the audit report.

We thank department personnel for their cooperation and assistance throughout the audit.

Respectfully submitted,

Scott A. Seacat
Legislative Auditor

Office of the Legislative Auditor

EDP Audit Report

Department of Labor and Industry

Members of the audit staff involved in this audit were Pete Brustkern, Ken Erdahl, and Frieda Houser.

Table of Contents

Appointed and Administrative Officials

Department of Labor and Industry	Laurie Ekanger, Commissioner
	Rod Sager, Administrator, Unemployment Insurance Division
	Joanne Loughney-Finstad, Chief, Benefits Bureau
	Sandra Bay, Chief, Contributions Bureau
	Wayne Schaff, Chief, Information Services Bureau
	Jon Moe, Chief, Administrative Services

Report Summary

Introduction

This is an audit of internal controls relating to the Department of Labor and Industry's computer-based Unemployment Insurance Benefits and Tax applications. We performed an electronic data processing audit of these applications. We selected the Department of Labor and Industry (DOLI) and these applications because of the significant dollar amounts that are processed and the widespread use of the information maintained on the systems.

General Controls

General controls are developed by the computer user to protect assets and limit losses. In our review of DOLI's general control environment, we found procedural controls to be adequate, but noted weaknesses in physical security and electronic access controls. We discuss these issues in Chapter II of the report and summarize them below.

Access Controls

Access controls provide electronic safeguards designed to ensure computer system resources are properly used. Logon IDs and passwords control electronic access to DOLI's computer applications, computer programs, and computer data. System and application programmers have the highest degree of technical expertise in the computer processing facility and, therefore, play an important role in maintaining the system. However, managers have the primary responsibility for maintaining adequate controls. Without adequate controls, computer specialists could alter program procedures and data for personal gain without leaving an audit trail.

Programmer Access Should be Restricted

The department's access rules give full (read, write, allocate, modify) privileges to all UI programmers for the UI applications. In addition, we found the contract programmers working on the new UI Tax application rewrite have unlimited access to all of the production programs and data entry screens for both the UI Tax and BeAR systems. Write access allows programmers to access and make unauthorized program changes or delete production programs and data. If unlogged, there is no record of programmer access.

Industry standards state programmers do not need access to system or application libraries which would provide a means of bypassing controls. Their activities should be restricted to test programs and files, with access only to those programs and files needed for a given assignment. At a minimum the programmer access should be logged and reviewed by department security personnel. Access by the contract programmers should be restricted, and any write access should be logged.

Terminated Employees' Access not Deleted in a Timely Manner

We found instances where the department did not follow established procedures to ensure terminated employees' access is suspended in a timely manner. We also identified five instances of access through terminated employees' IDs. This was addressed in a prior audit report, and the department agreed with our recommendation. However, we found instances department-wide where the problem still exists.

Use of Group User IDs Should be Limited

We found several user IDs assigned to a group of people, instead of an individual. Some of these IDs allow write access to the UI files. Electronic access guidelines recommend access to data files and programs be limited to those authorized to process and maintain specific systems. In addition, unique user IDs and passwords should be assigned to each user, rather than a group of users.

The sharing of user IDs and passwords makes it difficult to record each person's activities and establish individual accountability. This is especially critical when the ID has write access to production files. Shared IDs and passwords limit the confidentiality of information and increase the risk of unauthorized access to UI system data and programs.

Access Request Forms not Maintained

The department has policies in place which require an authorized "request for access" form be submitted to the security officer prior to access being granted for any user. The form is meant as a control to ensure only authorized and appropriate access is allowed to the UI systems. We found the control to be ineffective because access forms are not on file for many of the users, and of the ones we did find, many did not have the appropriate signatures authorizing the access.

ACF2 Reports Should be Reviewed

ACF2 software provides a daily report of logged user access to UI programs and data. In addition, the department receives a violation report which lists all unauthorized users who attempted to electronically access agency files. The agency security officer indicated he reviews the reports, but does not keep them for future reference. In order to ensure unauthorized access is not being obtained, another person other than the security officer should review the reports, and the reports should be retained for future reference.

Contingency Planning

Contingency planning is a basic element of safeguarding computer systems and information resources. A contingency plan should be comprehensive and periodically tested to facilitate an adequate recovery process. The contingency plan should include consideration of physical facilities, personnel, operating instructions, supplies and forms, application programs, documentation, system software, and data. It should be regularly updated to reflect changes in computer equipment and programs.

We reviewed the department's contingency plan to determine if it contained the minimum contingency guidelines as stated in section 1-0240.00, MOM. Our review indicated the plan is lacking in several areas. We noted the department's plan could be improved by:

1. Documenting backup recovery procedures.
2. Making provisions for backup hardware.
3. Documenting procedures for manual operation in the event of a disaster.
4. Providing a detailed definition of responsibilities for each organizational unit.
5. Identifying potential disasters and their impact.

Benefit Automation Rewrite

The UI Division operates a computerized application, the Benefit Automation Rewrite (BeAR) system that determines monetary and nonmonetary eligibility for unemployment benefit recipients, and tracks amounts paid for the various benefits programs. Input to the system is supplied by local Job Service personnel working with individuals requesting assistance. The system performs various tests to determine if the person is eligible for the requested benefits. The system determines the amount and duration of benefits to be distributed to a recipient and tracks the different types of benefits paid to the individuals during a given period. If the system indicates a discrepancy, it will prevent benefits from being paid, pending further fact-finding by UI personnel. If no problems are identified by the system, a benefit check is produced electronically and is mailed to the claimant. In fiscal year 1992-93, over $75.5 million in benefits were paid through the BeAR system.

We audited the BeAR system. Overall, we concluded controls over the system are adequate to ensure the accuracy and integrity of data on the system. However, we identified areas where controls could be enhanced to further ensure security and data integrity for the BeAR system. These issues are summarized below and discussed in Chapter III of the report.

Access to the BeAR System is not Adequately Controlled

The BeAR system has an access security system separate from the mainframe ACF2 system. The access security system is designed to restrict access to the various input screens. There are seven levels of access, each level granting access to several screens, including all screens designated in all of the lower levels. We found several users with access above that required in the performance of their jobs. This was partly due to being granted a level of access higher than necessary, and partly due to unneeded access within the level. This concern was addressed in a previous audit, where the department agreed there was a need for reprogramming the access system, but stated the cost and personnel required in the programming prevented them from following up on it. In 1992, department personnel estimated the cost to reprogram the system to further limit access to be approximately $19,000.

Wage Input Should be Double-Checked for Accuracy

When a claimant works part of his/her base year in another state and subsequently becomes eligible for unemployment insurance, he/she can file a Combined Wage Claim (CWC). This type of claim uses the wages from Montana and the other state(s) to determine the amount of benefits the claimant is entitled to. The CWC information is input manually by UI Benefits personnel. We identified instances where the information was not input accurately. A procedure for double-checking the accuracy of the information could prevent input errors from occurring.

Unnecessary Reports Printed and Distributed

Several daily, weekly, monthly, and annual reports are produced by the BeAR system and distributed within the UI Benefits Bureau. We found the checklist for the distribution of the reports was outdated, and the agency was relying on the distribution clerk to know where the reports were to be distributed. In addition, we determined several of the reports were being distributed but not used by anyone within the bureau. Some of the reports are recycled, while others are boxed and stored for a period of time. Bureau personnel should determine what information they need on the reports, and whether the present reports provide that information. They should then design specific reports to meet their needs and eliminate any unnecessary reports.

System Documentation Not-to-Date and Complete

Documentation provides a starting point for developing an accurate understanding of computer-processing activities and their impact on user groups. We found the system documentation for the UI applications is incomplete. In the event of programmer turnover, gaining an understanding of the system and its files and programs would be difficult without accurate and complete documentation. The department should update the documentation so it is useful to programmers and users, and develop procedures to ensure the documentation is kept updated with any changes or enhancements.

UI Contributions

Employers are required by federal law to participate in the unemployment insurance program. Individual employers make contributions to the program based on the amount of wages paid, the amount of UI benefits claimed by employees, and relative unemployment history of the occupation. The UI Contributions system, also known as the UI Tax system, is used to help identify those employers required to contribute to the system. It also calculates the rate employers are required to pay, based on information supplied by the employer, and tracks the collection of those taxes. The system resides on the state's IBM 3090 mainframe computer. Information is input by data entry personnel at the Contributions Bureau and is updated during a nightly batch update process.

We performed an application review of the UI Tax system, where we tested input, processing, and output controls. Overall, we concluded the controls in place were adequate and the system was operating effectively to ensure the accuracy and integrity of the data maintained on the system. However, we identified areas where controls could be enhanced to further ensure security and data integrity for the UI Tax system. These issues are discussed in Chapter IV and summarized in the following sections.

Combined Wage Claim Benefits not Charged Back to Employers

In order to be equitable in the calculation of employer tax rates, an employer's Unemployment Insurance tax rate is determined in part by a ratio of wages paid in the past three years compared to the amount of taxes paid less chargeable benefits paid to claimants since October 1981. Combined Wage Claim (CWC) benefits are paid by another state, and therefore the department does not input the claim into the BeAR system. Therefore, there is no mechanism to allocate CWC benefits to the Montana base period employer for experience rating purposes. In order to calculate the tax rate in a fair and equitable manner, the CWC benefits should be allocated to the individual employer.

Changes to Employer Tax Rate Should be Controlled

There are 17 data input screens for the UI Tax system which allow various data fields, such as name, address, employer number, tax rate and employer status to be updated. The

individual employer tax rate can be changed on three of these screens, with over 20 UI employees having access to these screens. Department personnel indicated only three people ever have any need to change the tax rate. The department should restrict access to the tax rate field to prevent accidental or intentional changes to the rate. Since the UI Tax system is in the process of being rewritten, the department should consider restricting the ability to change rates to only authorized personnel.

Chapter I - Introduction and Background

Introduction

This is an audit of internal controls relating to the Department of Labor and Industry's computer-based Unemployment Insurance Benefits and Tax applications. We performed an electronic data processing audit of these applications. We selected the Department of Labor and Industry (DOLI) and these applications because of the significant dollar amounts that are processed and the widespread use of the information maintained on the systems. In addition, this review provides assistance to the financial-compliance audit staff of the Legislative Auditor's Office in their biennial audit of the DOLI.

The Unemployment Insurance (UI) Division had approximately $75.5 million of expenditures and transfers out and $80.1 million of revenue and transfers in for fiscal year 1992-93. Federal funds are the source for $25.9 million of the division's revenue, employer contributions and premiums are the source for $47.2 million, and $7.0 million is investment income.

EDP Audit General and Application Controls

An Electronic Data Processing (EDP) audit consists primarily of a review of internal controls. In an automated environment the procedures for reviewing controls are different from those used in a manual environment. However, the objective of ensuring the reliability of controls is still the same. EDP auditing entails performing a general and an application control review. The general control review consists of an examination of the following controls:

Organizational - apply to the structuring and management of the data processing function. Specific types of organization controls include segregation of duties, assignment of responsibilities, rotation of duties, and supervision.

Procedural - operating standards and procedures which ensure the reliability of computer processing results and protect against processing errors.

Hardware and Software - controls within the operating system software and hardware which monitor and report system error conditions.

System Development - oversight and supervisory controls imposed on development projects. Controls include feasibility studies, development, testing and implementation, documentation, and maintenance.

Physical Security - physical site controls including security over access to the computer facility, protection devices such as smoke alarms and sprinkler systems, and contingency prevention and recovery plans.

Electronic Access - controls which allow or disallow user access to electronically stored information such as data files and application programs.

A general control review provides information regarding the ability to control EDP applications operating in the audited environment. Application controls are specific to a given application or set of programs that accomplish a specific objective.

Application controls consist of an examination of the following controls and objectives.

Input - Ensure all data is properly encoded to machine form and that all entered data is approved.

Processing - Ensure all data input is processed as intended.

Output - All processed data is reported and properly distributed to authorized individuals.

A review of the application documentation and audit trail is also performed. Applications must operate within the general controls environment in order for any reliance to be placed on them.

Background

The Department of Labor and Industry (DOLI) was created by the Executive Reorganization Act of 1971. DOLI enforces state and federal labor standards, enforces state and federal health-safety laws, conducts research and collects statistics that enable strategic planning, and provides adjudicative services in labor-management disputes. DOLI also operates as a part of a national employment, unemployment insurance (UI) benefits, and

training system that assists individuals in preparing for and finding jobs, assists employers in finding workers, and assists workers with benefits if they are temporarily unemployed through no fault of their own. There are seven types of UI benefits that can be paid to a qualified unemployed recipient:

Regular UI Benefits - are benefits paid from employer contributions to the UI system. Benefit duration ranges from 8 to 26 weeks.

Extended UI Benefits (EB) - is a special program created by the federal government to extend UI benefits beyond the monetary and duration limits of a regular UI claim. EB becomes effective when the unemployment rate reaches a certain level, and lasts for at least 13 weeks. (EB was not triggered during fiscal year 1993 or the first half of fiscal year 1994.)

Disaster UI Benefits (DUA) - is a special program for unemployment caused by an event declared a disaster by the President of the United States. (No DUA was triggered in Montana during fiscal year 1993 or the first half of fiscal year 1994.)

Emergency UI Benefits (EUC) - is a special program enacted by the U.S. Congress to extend unemployment benefits beyond the monetary and duration limits of the regular UI claim. (EUC benefits were distributed during fiscal year 1993 and the first half of fiscal year 1994.)

UCFE UI Benefits - are benefits paid from base period wages from federal agency civilian employment.

UCX UI Benefits - are benefits paid from base period wages from military employment.

Trade Readjustment Allowance Benefits (TRA) - was created by the Trade Act of 1974, amended in 1981. TRA is designed to pay additional benefits to claimants whose unemployment is caused by the increase of imported products which have caused a decline in the sales or production of a U.S. firm. TRA has been a fairly inactive program in Montana until recently. The shutdowns of the silver mine at Troy and the North American Free Trade Agreement are expected to increase the amount of benefits paid from this program.

DOLI maintains two primary computerized systems and several subsystems in the UI Division that collect historical employment

data, determine tax contribution rates for employers, and determine eligibility for unemployment benefit recipients. These systems also track amounts paid for Regular, Emergency, UCFE, UCX, and Extended Benefits. The two systems are:

Tax System - All employer contributions and quarterly wage information submitted by employers is entered to this system. The system also determines taxable rates for employers based on shared information from the Reserve Ratio System and the Benefit Automation Rewrite (BeAR) System.

BeAR System - All potential benefit recipients are entered to this system. The system shares information with the tax system to determine the amount, type, and duration of benefits to be distributed to a recipient and tracks the different types of benefits paid to individuals during a given period.

The UI Division systems are batch entry and update systems which operate on the mainframe computer maintained by the Department of Administration, Information Services Division (ISD). UI employees use mainframe terminals to perform programming and operations work. Eligibility technicians at local Job Service offices enter data into the UI Benefits system through personal computers. UI Tax system information is input centrally at the UI Division. The department is responsible for system recovery at the local level and relies on ISD to provide recovery for the mainframe.

Audit Objectives

The objectives of our EDP audit of the DOLI were to determine:

1. If the department is properly protecting and maintaining its computer-based information resources.
2. The adequacy of general controls, as they relate to the selected applications, including: procedural, physical security, and electronic access controls.
3. The adequacy of application controls over the Unemployment Insurance (UI) Benefits and UI Tax applications in order to evaluate the adequacy and accuracy of data processed and maintained by these applications.

Audit Scope and Methodology

The audit was conducted in accordance with government audit standards. We measured the department's general and application controls against criteria established by the American Institute of Certified Public Accountants (AICPA), General Accounting Office (GAO), and accepted industry EDP guidelines.

We reviewed the department's general controls related to the mainframe environment which processes the UI Benefits and UI Tax applications. We interviewed department personnel to gain an understanding of the hardware and software environment at the DOLI. We also reviewed available documentation relevant to the UI Benefits and UI Tax applications.

We conducted an application control review of the UI Benefits and UI Tax applications, as they operated through March 25, 1994. We reviewed:

1. Input controls, such as input authorization, edits, access controls, and error correction procedures.

2. Processing controls, including reconciliation procedures, processing edits, and recalculation of various formulas.

3. Output controls, such as report distribution procedures, and accuracy and validity of data on the reports.

We also determined if controls over data are effective as well as adequate to ensure the accuracy of data during processing phases.

Compliance

We determined compliance with state laws and federal guidelines applicable to the UI systems. Generally, we found the department to be in compliance with Unemployment Insurance requirements of Title 39, chapter 51, MCA. However, as discussed on page 15, we found the department is not in compliance with security requirements outlined in section 2-15-114, MCA.

Chapter II - General Controls

Introduction

Each year we review general controls over the state's mainframe computer at the Department of Administration during our Central Reviews audit. General controls are the procedures within a computer environment which ensure computer processing activities are controlled. We used the results of the fiscal year 1993 Central Reviews audit (93DP-33) for organizational, and hardware and system software controls, and did additional testing of physical security, procedural, and electronic access controls. The overall objectives of our general controls audit were to determine:

1. The adequacy of overall general controls operating over the UI systems.

2. The adequacy of procedural controls over system interfaces which ensure data is properly controlled and updated to the UI systems.

3. The adequacy of electronic access controls over UI system libraries, programs, files, data, and rate tables.

4. The adequacy of user control standards for access to the UI systems and verify user access is authorized.

5. Whether backup and disaster recovery procedures are established and reasonable to recover operations in the event of a disaster.

General controls are developed by the computer user to protect assets and limit losses. In our review of DOLI's general control environment, we found procedural controls to be adequate, but noted weaknesses in physical security and electronic access controls. We discuss these issues in the following sections.

Access Controls

Access controls provide electronic safeguards designed to ensure computer system resources are properly used. Logon IDs and passwords control electronic access to DOLI's computer applications, computer programs, and computer data. System and application programmers have the highest degree of technical expertise in the computer processing facility and, therefore, play an important role in maintaining the system. However, managers

have the primary responsibility for maintaining adequate controls. Without adequate controls, computer specialists could alter program procedures and data for personal gain without leaving an audit trail.

The state of Montana Information Technology Advisory Council has recently adopted guidelines for establishing electronic access controls for all computer system platforms. The guidelines are included in the Department of Administration's state computing directions, standards, and guidelines manual.

Proper access controls assist in the prevention or detection of deliberate or accidental errors caused by improper use or manipulation of data files, unauthorized or incorrect use of a computer program, and/or improper use of computer resources. The department's security officer writes rules which limit access to specific areas of the system. Assigning limited access based on job requirements facilitates checks and balances in the system. This approach prevents users from inadvertently or willfully executing programs or changing data unrelated to their job. We identified several areas where the department could improve its access controls. These are discussed in the following sections and on page 18.

Programmer Access Should be Restricted

Access to production files stored on the mainframe is protected by an application control package called Access Control Facility (ACF2). Rules are written which allow certain users to access specific data and/or programs. In addition, the UI application security systems further restrict access to specific screens within each system. We reviewed electronic access rights given to UI programmers for the UI programs and data. We found full (read, write, allocate, modify) privileges have been given to all UI programmers via ACF2. In addition, the programmers have full access to all UI screens through the application access security systems. Currently, this access is not logged or reviewed by department personnel.

Access to production files should be limited to those authorized to process or maintain particular systems. In addition, no one person should have access to write information to both programs

and data. A person with unrestricted access could modify the existing programs and/or data without authorization and potentially manipulate the system.

Access to production files should be limited based on the job duties of individual personnel. Ideally, write access to production files should be limited to the person performing a particular job, and only for the time period needed to complete the job. Department personnel indicated programmers have write access to the production files for the purpose of production recovery during the nightly batch update. However, the access should be restricted to read only, except for the programmer on call for the night.

The department should examine alternative methods for ensuring appropriate access to production files. If production recovery necessitates access by the programmers, the reason for the access should be documented and the access should be limited to specific time periods. At a minimum the access should be logged and reviewed by department security personnel.

Recommendation #1

We recommend the department:

A. Restrict programmers to read only access to production files, except as documented, and

B. Log and review all programmer access to production programs.

Contract Programmers' Access Should be Restricted

During our review of access controls, we found the contract programmers working on the new UI Tax application rewrite have unlimited access to all of the production programs and data entry screens for both the UI Tax and BeAR systems. The same potential for unauthorized manipulation of the system exists as was noted for UI programmer access. Department personnel

indicated the contract programmers need access to all of the production programs in order to perform their duties in the creation of the new system. However, the new system is being created in a test environment and the programmers should not need access to either production system until the final product is ready for implementation.

As a result of our finding, the department has begun to log the contract programmers' access on ACF2 for reference in case anything questionable is identified. However, we believe the unlimited access should be deleted, and access be given to the contract programmers only on a limited basis as authorized.

Recommendation #2

We recommend the department restrict the contract programmers' access to production programs.

Terminated Employees' Access not Deleted in a Timely Manner

During our review we found instances where the department did not follow established procedures to ensure terminated employees' access is suspended in a timely manner. We also identified five instances of access through terminated employees' IDs.

We reviewed system security files for personnel who had their security access suspended within the last year. We found 15 out of 32 terminated personnel whose access was still active at least two weeks after their employment with the department ended. Of the 15 people, 10 still had access at least two months after termination. When terminated employees' access is not suspended, unauthorized use or alteration of data and programs could occur. For example, we found six logon IDs were used to access the computer system after the personnel who were assigned the logon IDs had terminated their employment with the department. Department personnel could not explain the unauthorized access for five of these employees.

In a prior audit report we recommended the department suspend terminated employees' access to computer systems and data on a timely basis. The department concurred with the recommendation. Department personnel stated it has been the responsibility of the division administrators to notify the security officer of terminated employees, and without their cooperation the security officer could not suspend access in a timely manner.

The UI security officer indicated she has recently developed procedures which require monthly reports from the Personnel Bureau, to inform her of employee terminations. In addition, she has begun sending annual notices to non-DOLI agencies requiring them to indicate any terminations or needed changes in access levels. We believe these procedures could reduce the risk associated with untimely suspension of employee access. However, the procedures should be documented in a formal policy to help ensure the procedures are followed.

Recommendation #3

We recommend the department document the procedures for timely suspension of access to its computer systems and ensure the procedures are followed.

Use of Group User IDs Should be Limited

The department maintains several group user IDs for the Job Service Division personnel. These IDs are designed to allow users in the division to share a terminal without needing to log on and off each time. Individuals using these IDs have write access to the BeAR system. Another group user ID is used by computer operations personnel. This ID was created for testing within the computer operations section. Individuals using this ID have unlimited access to all production programs and files. Department officials indicated this ID is no longer used and will be suspended.

Electronic access guidelines recommend access to data files and programs be limited to those authorized to process and maintain specific systems. In addition, unique user IDs and passwords should be assigned to each user, rather than a group of users. Assigning individual user IDs and passwords increases the level of system security and assigns accountability and responsibility.

The sharing of user IDs and passwords makes it difficult to record each person's activities and establish individual accountability. This is especially critical when the ID has write access to production files. Shared IDs and passwords limit the confidentiality of information and increases the possibility of a change to data and programs. The use of group user IDs increases the risk of unauthorized access to BeAR system data and programs. Such access would not be traceable to one individual.

Department personnel indicated they will weigh the risks of the use of group IDs with the ability to efficiently serve the customer, and delete unnecessary access through group IDs.

Recommendation #4

We recommend the department establish and implement policies which limit the use of group IDs to inquiry access only.

Access Request Forms not Maintained

We found 476 DOLI and other agency employees have some level of access to the UI Tax application. The department assigns various levels of access to information based upon the employee's position in the department. Contributions Bureau employees, for example, can review and update information in the employer files, but individuals in agencies outside the department are allowed inquiry only access to the information.

The department has policies in place which require an authorized "request for access" form be submitted to the security officer prior to access being granted for any user. The form is meant as a control to ensure only authorized and appropriate access is allowed to the UI systems. During our review we tested twelve users and found the access request forms are not on file for six of them. For those users, we could not determine if access was authorized or if the allowed access was reasonable. Of the ones we did find, many did not have the appropriate signatures authorizing the access.

Industry standards recommend management limit user access to data files required to process or maintain particular applications in the performance of their duties. Use of the access request forms reduces the risk of unauthorized and/or inappropriate access to the UI systems. Use of the forms should be required of all personnel requesting access.

Department personnel stated the security function has been assigned to different people over the last few years, and therefore it has been difficult to maintain consistent enforcement of standard security policies. They also stated the access request forms were not required until 1989, so access granted prior to that time would not have supporting documentation.

To improve access controls, we believe the department should establish access review procedures. For example, the department should require department supervisors to review current employees' access levels to determine if access needs have changed, and are reasonable. In order to be effective, these access review procedures should be performed every six months to a year.

Recommendation #5

We recommend the department:

A. Enforce the current policies requiring access request forms for all access granted, and

B. Develop procedures for periodic review of access levels for reasonableness.

ACF2 Reports Should be Reviewed

ACF2 software provides a daily report of logged user access to UI programs and data. In addition, the department receives a violation report which lists all unauthorized users who attempted to electronically access agency files. The department security officer reviews these ACF2 reports to monitor who accesses which program libraries and to determine whether access is authorized. We determined the department's security officer is the only individual who reviews ACF2 violation reports. In addition, the reports are not retained for future reference. Retention of the reports would aid in the internal security review, as discussed on page 14, and provide an audit trail should problems be identified relating to inappropriate access.

The security officer has unlimited access to software and data files. A security officer can access, change, or delete programs and data without detection. An individual outside of the security and data processing environment, preferably from a user group, should review ACF2 reports in addition to the security officer. An independent review provides more effective access control by reviewing access violations, programmer activity, and changes made by security.

Without an independent review, the potential exists for inappropriate access and unauthorized changes to UI data and programs. We discussed our finding with department officials. The officials were not aware potential control weaknesses exist but

have agreed to perform independent reviews of ACF2 reports and retain the reports.

Recommendation #6

We recommend the department:

A. Establish procedures for an independent review of ACF2 reports.

B. Retain the ACF2 reports for future reference.

Internal Evaluations of Security

We determined the department does not perform internal evaluations of security in accordance with state law. Section 2-15-114, MCA, requires department heads to be ". . . responsible for assuring an adequate level of security for all data and information technology resources within his department and shall . . . (4) ensure internal evaluations of the security program for data and information technology resources are conducted."

The department should establish policies and procedures in accordance with state law which address safeguarding data and information technology resources including microcomputer policies and program documentation. As defined in state law, these procedures include, but are not limited to, the following:

1. Conduct and periodically update a comprehensive risk analysis to determine security threats to data and information resources.

2. Develop and periodically update written policies and procedures which provide security over data and information resources.

3. Implement appropriate cost-effective safeguards to reduce, eliminate, or recover from identified risks to data and information resources.

4. Perform periodic internal audits and evaluations of the security program for data and information resources.

We believe the electronic access control issues discussed on pages 7 through 14 resulted because the department does not have formal policies and procedures for internal evaluations of security.

Recommendation #7

We recommend the department develop and implement policies and procedures for internal evaluations of security in accordance with state law.

Contingency Planning

Contingency planning is a basic element of safeguarding computer systems and information resources. Contingency planning involves collecting plans, procedures, arrangements, and information which are completed, compiled, and held in readiness for use in the event of a disruption of normal activities. A contingency plan should be comprehensive and periodically tested to facilitate an adequate recovery process. The contingency plan should include consideration of physical facilities, personnel, operating instructions, supplies and forms, application programs, documentation, system software, and data. It should start with an inventory of equipment and programs and be regularly updated to reflect changes in computer equipment and programs.

Since the UI systems are run on the state's mainframe computer, files and programs are backed up regularly by the Department of Administration's Information Services Division, and provisions have been made for the replacement/repair of the mainframe equipment. However, the department is responsible for ensuring a contingency plan is in place for all equipment and supplies located at the DOLI offices.

We reviewed the department's contingency plan to determine if it contained the minimum contingency guidelines as stated in

section 1-0240.00, MOM. Our review indicated the plan is lacking in several areas. We noted the department's plan could be improved by:

1. Documenting backup recovery procedures.

2. Making provisions for backup hardware.

3. Documenting procedures for manual operation in the event of a disaster.

4. Providing a detailed definition of responsibilities for each organizational unit.

5. Identifying potential disasters and their impact.

The department's use of computers is critical to the operation of the UI Division. Loss of computer use would significantly impact department operations. The department has discussed many of the options and solutions for recovering from a disaster or other disruption of normal activities, and began to document a plan several years ago. However, because of time constraints, the plan was never completed and has not been updated.

A written, detailed plan outlining recovery procedures should exist and be tested to ensure feasibility of the plan. We recognize thorough contingency planning is an intensive and on-going process. However, maintaining an adequate contingency plan will ensure continued data processing operations and the department's compliance with section 1-0240.00, MOM.

Recommendation #8

We recommend the department:

A. Establish a formal contingency plan in compliance with section 1-0240.00, MOM.

B. Periodically test the contingency plan.

Chapter III - Benefit Automation Rewrite System

Introduction

The UI Division operates a computerized application, the Benefit Automation Rewrite (BeAR) system that determines monetary and nonmonetary eligibility for unemployment benefit recipients, and tracks amounts paid for the various benefits programs. Input to the system is supplied by local Job Service personnel working with individuals requesting assistance. The system performs various tests to determine if the person is eligible for the requested benefits. If the system indicates a discrepancy, it will prevent benefits from being paid, pending further fact-finding by UI personnel. If no problems are identified by the system, a benefit check is produced electronically and is mailed to the claimant. In fiscal year 1992-93, over $75.5 million in benefits were paid through the BeAR system.

All potential benefit recipients are entered into the BeAR system. The system collects wage information for recipients from the UI Tax system for Montana employers and the INTERNET system for out-of-state employers. The system determines the amount and duration of benefits to be distributed to a recipient and tracks the different types of benefits paid to the individuals during a given period. Information is entered to the system daily at DOLI and local Job Service offices throughout the state. The newly entered information resides in a transaction file until a nightly batch update job is run. During the batch update, benefit and wage master files in the BeAR system are updated by information from the transaction file.

We conducted an electronic data processing audit of the BeAR system. Overall, we concluded controls over the system are adequate to ensure the accuracy and integrity of data on the system. However, we identified areas where controls could be enhanced to further ensure security and data integrity for the BeAR system. This chapter discusses our findings from our audit of the BeAR system.

Access to the BeAR System is not Adequately Controlled

As discussed in Chapter II, the BeAR system has a separate access security system. The access security system is designed to restrict access to the various "screens." The screens are generated through individual computer programs, and range from initial claim information, input from the UI claim form, to inquiry only screens which summarize claims and payments to an individual. Also, there are several screens which allow correction and update of initial information. Information on the screens includes such things as name, address, social security number, eligibility status, and child support information. Various levels of access are designated for the screens, based on their criticality. Level one, for instance, gives access only to inquiry screens, while level seven gives access to all screens, both inquiry and input. There are presently seven levels of access and access is cumulative. If a person has level six access, for instance, he would have access to the screens specified in level six and would also have access to everything specified in levels one through five.

We reviewed all UI Division employees with the highest levels of access, levels six and seven. Of the 17 tested, 10 needed only level five or lower access. We also interviewed several Job Service personnel with level five access, and found they only needed level three access to perform their job duties. In addition, we tested all personnel outside the UI Benefits Bureau who had access above level one, which is inquiry only, and found 8 of 31 had access over what was required for the performance of their jobs.

Access to information should be restricted to personnel needing that access in the performance of their jobs. Inappropriate access could result in accidental or intentional manipulation of the UI data.

Agency personnel indicated the improper access occurred partly because of employees needing temporary access to certain screens, and the access not being reduced once the need is over. Also, employees may need access to only one screen in an access level, but because of the way the access system is set up, the

employees receive access to several additional screens not necessary for their job.

A periodic management review of the access levels given to individuals could prevent improper access from continuing for an extended period of time. In addition, the system security program could be revised to restrict access on a per-screen basis. This was addressed in a previous audit, where the department agreed there was a need for reprogramming the access system, but stated the cost and personnel required in the programming prevented them from following up on it. In 1992, department personnel estimated the cost to reprogram the system to further limit access to be approximately $19,000.

Recommendation #9

We recommend the department:

A. **Periodically review BeAR system access given to all individuals.**

B. **Determine the feasibility of reprogramming the security system to restrict access on a per-screen basis.**

Wage Input not Double-Checked for Accuracy

When a claimant works part of his/her base year in another state and subsequently becomes eligible for unemployment insurance, he/she can file a Combined Wage Claim (CWC). This type of claim uses the wages from Montana and the other state(s) to determine the amount of benefits the claimant is entitled to. The wage information from the other state(s) is received at the UI Benefits Bureau via INTERNET, on an IB4 form. The wage information, broken down by employer and wages per quarter, is then input manually to the BeAR system.

We reviewed 12 CWC forms to determine if the information was input accurately and completely, and found one where the information had been input incorrectly. The mistake caused the claimant to receive benefits of $174 per week when he should have received $187 per week. Over the ten week period of eligibility, the claimant was shorted a total of $130. With over 3,000 CWC forms filed annually, the total dollar amount of all input errors could be significant.

Department personnel indicated they have identified other errors where a control of double-checking or verifying the input may have prevented the errors. Personnel indicated with the relatively low number of CWC forms input each year, a double-check procedure would be feasible. However, they have not yet implemented such a procedure.

Recommendation #10

We recommend the department implement procedures to verify the accuracy of all CWC information input to the BeAR system.

Unnecessary Reports Printed and Distributed

We reviewed reports produced by the BeAR system and distributed within the UI Benefits Bureau. The bureau uses a checklist to aid in the distribution of the reports. We found the names on the checklist were not kept updated when changes were made in staffing. In addition, of the 22 reports we reviewed, we found 10 that are not used. Some of the reports are recycled immediately, while others are retained and stored for extended periods of time. For instance, the check register report is kept on a shelf for a few days and then recycled, and is not reviewed by anyone. The summary of the check register has erroneous information and department personnel could not explain why the information was incorrect. With some other reports, the

employees could not explain where the information comes from or what it might be used for.

The printing and storing of unused reports is an unnecessary expense and requires additional time from bureau personnel for handling and processing of the reports. Department personnel indicated the issue of unused reports has been discussed at staff meetings, but several unused reports are still produced.

Since the inception of the BeAR system, the information needs of the UI Bureau may have changed, and information that was useful then may not meet its needs now. Therefore, bureau personnel should determine what information they need on the reports, and whether the present reports provide that information. They should then design specific reports to meet their needs and eliminate any unnecessary reports.

Recommendation #11

We recommend the department:

A. Update the report distribution checklist to reflect changes in staffing, and

B. Reevaluate the reports presently generated and eliminate any unnecessary reports.

System Documentation not Up-to-Date and Complete

Documentation provides a starting point for developing an accurate understanding of computer-processing activities and their impact on user groups. System documentation generally provides:

1. An understanding of a system's objectives, concepts, and output.

2. A source of information for systems analysts and programmers who are responsible for maintaining and revising existing systems and programs.

3. Information necessary for supervisory review.

4. A basis for training new personnel.

5. A means of communicating common information to other system analysts, programmers, and operators.

6. A source of information about accounting controls.

7. A source of information needed to provide continuity in the event of loss of experienced personnel.

We interviewed programming personnel and reviewed available manuals to determine if system documentation exists for the BeAR system and is adequate to define the system, programs, files, etc. We found some of the documentation to be current, such as record definitions and INTERNET code. However, the internal and external design manuals had not been updated since the inception of the BeAR system in 1985. Also, documentation of programs and datasets and their interrelationships was not available.

Agency personnel indicated they realize the need to update the documentation but time and personnel restrictions have caused the project to be "put on the back burner."

In the event of programmer turnover, gaining an understanding of the system and its files and programs would be difficult without the benefit of accurate and complete documentation. The department should update the documentation so it is useful to programmers and users, and develop procedures to ensure the documentation is kept updated with any changes or enhancements.

Recommendation #12

We recommend the department:

A. Update the BeAR system documentation.

B. Establish policies and procedures to ensure future changes to the system are included in the documentation.

Chapter IV - Unemployment Insurance Contributions System

Introduction

Employers are required by federal law to participate in the unemployment insurance program. Individual employers make contributions to the program based on the amount of wages paid, the amount of UI benefits claimed by employees, and relative unemployment history of the occupation. The UI Contributions system, also known as the UI Tax system, is used to help identify those employers required to contribute to the system. It also calculates the rate employers are required to pay, based on information supplied by the employer, and tracks the collection of those taxes. The system resides on the state's IBM 3090 mainframe computer. Information is input by data entry personnel at the Contributions Bureau and is updated during a nightly batch update process.

We performed an application review of the UI Tax system, where we tested input, processing, and output controls. Overall, we concluded the controls in place were adequate and the system was operating effectively to ensure the accuracy and integrity of the data maintained on the system. However, we identified areas where controls could be enhanced to further ensure security and data integrity for the UI Tax system. These issues are discussed in the following sections.

Combined Wage Claim Benefits not Charged Back to Employers

When an unemployment insurance claim is made, and the claimant is receiving benefits entirely from Montana base period wages, the benefits paid are charged back to the employer's account. This information is then used in the calculation of the following years' contribution rates for that employer.

As discussed in chapter III, employees who earn wages in Montana and then move to another state can claim Unemployment Insurance benefits using the Montana wages in their base wage calculations. The benefits are paid by the state of residency, but Montana must then reimburse that state for its share of benefits paid. This is called a Combined Wage Claim (CWC) and can include two or more states. During our review, we found CWC benefits paid were not allocated to the Montana employer for experience rating purposes.

In order to be equitable in the calculation of employer tax rates, an employer's Unemployment Insurance tax rate is determined in part by the benefits charged to their account since October 1, 1981. Since the CWC benefits are paid by another state, the department does not input the claim into the BeAR system. Therefore, there is no mechanism to allocate CWC benefits to the Montana base period employer for experience rating purposes.

In 1986, the department performed a Benefit Charging Study and estimated there were $2 million in CWC payments that were not allocated to Montana employers in 1985 for experience rating purposes. Another study in 1994 estimated allocable benefits in 1993 to be approximately $978,000.

As a result of CWC payments not being charged back, Montana employers who had claimants move to another state and use the base wages earned in Montana may have been assessed a lower UI tax rate than they would have been charged if the CWC benefits paid out were tracked by Montana. Because of the lower rates for individual employers, the statewide rate would be increased to compensate. In order to calculate the tax rate in a fair and equitable manner, the CWC benefits should be allocated to the individual employer.

Department officials stated the reason these benefits are not charged to the employers is the cost to implement the necessary program changes. At the present time, UI programmers have not set this as a priority. We estimated the programming changes to incorporate the CWC payments into the employer charge-back calculation would take approximately 1100 programmer hours, at a cost of approximately $38,000.

Recommendation #13

We recommend the department develop a plan to implement programming changes to include CWC benefits in the UI tax rate calculations.

Changes to Employer Tax Rate Should be Controlled

There are 17 data input screens for the UI Tax system which allow various data fields, such as name, address, employer number, tax rate and employer status to be updated. The individual employer tax rate can be changed on three of these screens, the E-4 Rating Entry screen, the CH Change Entry screen, and the E-1 Status Entry screen. Over 20 UI employees have access to these screens, which gives them access to change the tax rate. Department personnel indicated only three people, all in the Contributions Bureau, ever have any need to change the tax rate and access could be restricted to those three people.

The ability to change the tax rate by people who are not authorized to make the changes could result in intentional or accidental changes to the rates and result in incorrect taxes being charged to the employers. As a compensating control, a "Rate Discrepancy Report" is printed by the system and distributed to contributions personnel for review. However, the report is not retained for future reference.

Since the UI Tax system is in the process of being rewritten, the department should consider restricting the ability to change rates to only authorized personnel. Authorized changes to the rates are recorded and filed in the employer's file. In order to ensure all changes are authorized, however, the rate discrepancy report should be reviewed and retained for a specified period of time, such as six months to a year.

Recommendation #14

We recommend the department:

A. Ensure only authorized personnel have access to change employer tax rates.

B. Retain the rate discrepancy reports for a specified period of time.

Agency Response

DEPARTMENT OF LABOR AND INDUSTRY

COMMISSIONER'S OFFICE

MARC RACICOT, GOVERNOR

P.O.BOX 1728

STATE OF MONTANA

(406) 444-3555
FAX (406) 444-1394

HELENA, MONTANA 59624

June 6, 1994

Scott A. Seacat
Legislative Auditor
Office of the Legislative Auditor
State Capitol
Helena, MT 59620

Dear Scott:

Attached is our response to the recommendations contained in the draft EDP Audit Report on the Unemployment Insurance Division applications, dated June 1994.

We appreciate the cooperative spirit of the audit staff in the discussion of concerns raised and possible solutions. Also, we especially appreciate the independent look at security aspects of this operation because it affords us the opportunity of identifying problems that are sometimes unseen by those closest to the problems.

Although, in some instances, the concerns are raised in the context of the audit of the Unemployment Insurance Division application controls, the issues raised will be addressed by this department, where appropriate, as department-wide issues to ensure the uniformity of policy and procedures.

The Unemployment Insurance Division staff and I will continue to be available to work with you and the Legislative Audit Committee to answer questions about the audit and our response.

Thank you for your help.

Sincerely,

Mark Blend

for LAURIE EKANGER
Commissioner

LE:ka

RECOMMENDATION # 1

We recommend the department:

A. Restrict programmers to read only access to production files, except as documented.

AGENCY RESPONSE - Partially concur. We agree that access by U.I Division programmers to files of other divisions should be restricted, but do not agree that U.I. programmers be restricted to read only access to the U.I files. Programmers routinely need more than just read access to production files. There are times when a programmer is the only person around to execute a procedure for a user. The programmers primary job is to produce required data and/or reports under strict timelines for the Department's needs. Therefore, ACF2 rules are in place or will soon be in place to restrict U.I. programmers to U.I. files only. UI programmers will not be able to get into Job Service data sets and visa versa. In addition, we will implement a change to ACF2 rules to log the U.I. programmers when they update the U.I. production files.

B. Log and review all programmer access to production programs.

AGENCY RESPONSE - Concur. We will modify ACF2 rules to cause a log entry anytime a programmer updates a production program, thereby creating an audit trail as to who updated production programs and when. The Information Services Bureau Chief has implemented a routine review of the access log by a separate person (computer operator technician) from his office, with instructions that questionable entries be reported to the security officer.

RECOMMENDATION # 2

We recommend the department restrict the contract programmers' access to the production programs.

AGENCY RESPONSE - Concur. Contract programmers do require access to production programs (there are only two contract programmers working for the department at this time and they are doing work for the UI Division). At the current time if one of the contract programmers does access production programs or production data files, ACF rules are in place to log the occurrence and report it on the "Daily Access Log." We placed some additional restrictions on the contract programmers when the concern was brought to our attention by the EDP auditor.

The contract programmers currently installing a new tax system for U.I. have full ACF access only to datasets specifically set up for their use in installing the new system (identified by the first two nodes F22.D250). They have read access to our current production datasets but are logged by the ACF rules if they try updating them. These log messages will appear on the daily ACF reports.

This read access is necessary to allow them to carry out the functions of their job. These include reading the old master file for conversion to the new format (which just recently was added to the scope of their responsibilities), pulling pieces out of the old system code and retooling them to the new system, and executing modules in the existing U.I. systems which will be retained for the new system.

In addition, it should be noted that, when entering into the contract, a large performance security was required of the contractors and they were required to carry $600,000 in liability insurance. The contract also contains language requiring the contractor to withhold information on individual claimants and employers.

RECOMMENDATION # 3

We recommend the department document the procedures for timely suspension of access to its computer systems and ensure the procedures are followed.

AGENCY RESPONSE - Concur. We strongly agree that access by terminated employees to department computer systems must be suspended in a timely manner upon termination. We also agree that procedures for suspending access of terminated employees need to be documented and strictly followed. Based on the concern raised, we are reviewing our policy and procedures to ensure that the appropriate steps are taken in a timely and efficient manner to protect the integrity of department systems. We expect to have documentation of policies and procedures complete by September 1, 1994. Our efforts in this regard shall ensure the maintenance of adequate documentation of the policy and related procedures and ongoing emphasis to management and security personnel of the importance of suspending access of terminated employee on a timely basis. Just prior to the audit, we changed internal controls to assure that suspension of access to the benefits system and the tax system is coordinated. We also instituted a new form to coordinate personnel changes with our budget officer since they are usually the first to receive relevant documentation.

RECOMMENDATION # 4

We recommend the department establish and implement policies which limit the use of group IDs to inquiry access only.

AGENCY RESPONSE - Concur. We agree that use of group I.D.'s should be limited to circumstances in which their use is necessary and we are in the process of reviewing their use in the department. We are cognizant of the risks involved in the use of a group I.D. number, but must also weigh the risk in relation to our ability to efficiently serve the customer.

For our review of group I.D. usage, we requested the list of group I.D. numbers identified by the auditor and are reviewing the use of those I.D. numbers. It has already become apparent that many of the identified I.D. numbers do not access U.I. files, but from a department perspective, we will still assess the need for them. By September 1, 1994, we will document what U.I. related group I.D.'s need to be retained and for what purpose. Others will be eliminated.

RECOMMENDATION # 5

A. Enforce the current policies requiring access request forms for all access granted.

AGENCY RESPONSE - Concur. Current policies have been enforced in recent years. However, the audit identified persons having access authorized prior to the implementation of current policies and their access authority was not documented by the then implemented access forms. The procedure for periodic review (below) will update the access documentation for those people.

B. Develop procedures for periodic review of access levels for reasonableness.

AGENCY RESPONSE - Concur. We are in the process of developing a procedure for periodic review of access levels. A form has been designed that will identify for each CE number, or position number, the degree of access needed, and this form will be used as a reference in future periodic reviews. This procedure will be implemented in the near future. Our goal is to have forms documenting the authorized level of access of all division employees within a year.

RECOMMENDATION # 6

We recommend the department:

A. Establish procedures for an independent review of ACF2 reports.

AGENCY RESPONSE - Concur. As mentioned for recommendation #1, we have established a routine review of the ACF reports by the computer operator technician who will report questionable log entries to the department security officer. The criteria for this review procedure has been developed and implemented by the Information Services Bureau Chief.

B. Retain the ACF2 reports for future reference.

AGENCY RESPONSE - Concur. The department security officer has established a policy that we maintain the daily ACF2 reports for one (1) year from the day they are printed.

Any questions that we have on these reports are noted on the report as to who we contacted concerning the "LOG" and/or "VIOLATION," what the reason was for the "LOG" and/or "VIOLATION" and what we did about it to remedy the situation so it doesn't happen again.

RECOMMENDATION # 7

We recommend the department develop policies and procedures for internal evaluations of security in accordance with state law.

AGENCY RESPONSE - Concur. The absence of formal policies and procedures related to internal evaluation of automated systems security issues is a valid concern. It does not, however, reflect an accurate view of the current environment. Risk assessments performed for our federal counterpart review security issues of the U.I Division. Also, we believe that the security of U.I. programs and data is evaluated and maintained through various safeguards currently in place in the division (plus some to be added based upon recommendations above), but documentation is indeed lacking. There are a couple of reasons why this occurs. First, the development of such documentation is always cumbersome to prepare but is even more cumbersome to maintain, and this takes considerable resources which are spread thin already. Second, the changes in technology over even the shortest of time frames tends to make such documentation obsolete very quickly. While these are obvious excuses for a real concern, the department is committed to improving its documentation of the policies and procedures applied in maintaining the integrity of department systems, and will continue efforts to formalize an internal evaluation of security

provisions. We have set a target of January 1, 1995, to document the existing policies and procedures and those which will be implemented by that date.

RECOMMENDATION # 8

We recommend the department:

A. Establish a formal contingency plan in compliance with section 1-0240.00.MOM.

AGENCY RESPONSE - Concur. We are reviewing the extent to which Unemployment Insurance Division mainframe programs and data are included in the Department of Administration contingency plans. Specifically, we will identify which parts of the U.I. systems have been identified as critical applications in the context of Section 1-0240.00 of the Montana Operations Manual.

However, we agree that the documentation of contingency plans is inadequate, although The U.I. Division has periodically reviewed contingency measures as part of risk assessments that are performed under federal requirements. There are also some limited policy statements, in the department policy manual, related to use of computers, ownership of software, and documentation and backup of systems on personal computers. Overall, we agree that formal documentation of U.I. Division contingency plans is not adequate and this shortcoming will be addressed in the future as resources become available. The continued development of a contingency plan has been included in the list of projects to be defined and addressed by the Administrative Services Bureau.

B. Periodically test the contingency plan.

AGENCY RESPONSE - Concur. The contingency plan will include a periodic test procedure.

RECOMMENDATION # 9

We recommend the department:

A. Periodically review BeAR system access given to all individuals.

AGENCY RESPONSE - Concur. We will periodically review BeAR system access to keep access current.

We agree that tighter security is desirable to control accidental access although there have been no incidents of intentional manipulations of data identified since the BeAR was implemented in August of 1985. The possibility of human error exists at any level of security but erroneous data entry due to unauthorized access has not been identified as an issue.

We disagree with the exception to level 5 security being assigned to Job Service staff. Job Service began adjudicating certain non-monetary issues in 1989 in the interest of better customer service. The screens for non-monetary resolution require level 5 security.

Annual reviews were initiated to keep the internal user community current and security access at the appropriate level and we will make it a priority to maintain this process in the future. Over the past year we have made a change to our security policy to tighten system access. We have instituted a policy of position-specific access, and have begun the documentation process. The documentation of each position is projected to be complete by October 1, 1994.

We agree that a periodic review of the BeAR access should be given on all individuals. Each year UI updates the information sharing agreements with the participating agencies. At that time, UI sends a list of all users that are authorized to use UI information from that agency. An on-site review would tighten that review and is part of this year's risk plan.

Internal employee verifications are currently conducted annually.

B. Determine the feasibility of reprogramming the security system to restrict access on a per-screen basis.

AGENCY RESPONSE - Partially Concur. We will continue to study the cost-benefit of reprogramming the security system to restrict access on a per-screen basis. It is not cost effective at this time since no abuse has been identified. The issue remains on our request for programming list and will be a part of any system rewrite in the future.

RECOMMENDATION # 10

We recommend the department implement procedures to verify the accuracy of all CWC information input to the BeAR system.

AGENCY RESPONSE - Partially concur. We agree with the concern of possible human error when manually data entering wage amounts from IB-4 information transferred over the Internet System. We do not agree that this is a universal problem but an isolated incident.

It is the **normal procedure** for staff to verify that total wages agree with the amount transferred. The monetary determination sent to the claimant advises them to verify the accuracy of the wage information as well because wages are often misreported by the employer and the agency has no way of identifying these types of errors. If there are wage discrepancies for any reason, the claimant would normally identify them. We believe very few errors go undetected.

To implement a double-checking procedure, we would have to hire another person, at least during heavy volume periods. While recent years have seen additional funding (contingency funds) available for increased volume (related to Emergency Unemployment Compensation Act in past winter), it appears that these funds are on the decrease.

This potential problem should be eliminated with the implementation of an automated interface between the IB-4 process and the wage file. We have been unable to dedicate agency staff to this interface, however we have accepted an offer of assistance from Martin-Marietta, the Internet contractor in Orlando, Florida, to install an interface used in several states, customized to Montana's requirements. They have several implementations scheduled and Montana is on the waiting list. They estimate that the interface will be installed in Montana within the next year.

RECOMMENDATION # 11

We recommend the department:

A. Update the report distribution checklist to reflect changes in staffing.

AGENCY RESPONSE - Concur. We have had considerable turnover in the last few months and the list was not updated pending filling the vacant positions however as soon as staff becomes static, the list will be revised. Staff who distribute the reports know where the reports go based on duties assigned to the positions rather than names of person in the position.

B. Reevaluate the reports presently generated and eliminate any unnecessary reports.

AGENCY RESPONSE - Concur. We agree the reports should be reviewed periodically. We do review the printed reports regularly. We eliminate some reports that are not used or required and microfiche others when the information is required to be retained for any length of time.

We believe this process is currently in place and has been since the automated system was implemented. We do not agree this is an exception.

We normally poll the staff both in Central Office and Job Service to ensure we do not eliminate a necessary report. We have recently eliminated several reports which possibly include some of the ones identified by the audit.

The check register is not immediately recycled, it remains in our Benefit Support Unit for a short period to ensure that any obvious errors are resolved before being destroyed. Discrepancies in summary information and system problems with checks are usually reviewed by the Bureau Information Systems Support Specialist, who was not contacted with this concern. The check register is available on microfiche for future reference.

The support specialist would also be able to explain where information comes from in most instances and if not, obtain the information from the system programmers. Again, the appropriate staff person was not contacted with this concern. Also, one of the supervisors could have assisted auditors in tracking source information or direct them to appropriate staff.

We will continue to review the reports for possible elimination based upon the cost to print and store. We will eliminate any of the ones identified as "not used" after verifying with all staff that they are obsolete. We will cease printing those that do not require a hard copy.

RECOMMENDATION # 12

We recommend the department:

A. Update the BeAR system documentation.

AGENCY RESPONSE - Concur. We agree with this concern. We intend to update documentation and ensure future changes to the system are included in the documentation. Lack of documentation has been identified as an universal industry problem and this concern has been addressed in training sessions with programming staff.

It is possible that if additional automation funding is received we will be able to dedicate staff to this task. We are definitely concerned with the possibility of loss of expertise rendering the system ineffective and have been aware that this potential exists. It should be noted that changes to system programs are documented in the programs themselves. The concern is with the system's manuals which do not get routinely updated.

B. Establish policies and procedures to ensure future changes to the system are included in the documentation.

AGENCY RESPONSE - Concur. As indicated above, we are committed to ensuring that future system changes are adequately documented.

RECOMMENDATION # 13

We recommend the department develop a plan to implement programming changes to include CWC benefits in the UI tax rate calculations.

AGENCY RESPONSE - Partially Concur. We agree that the absence of the ability to charge back benefits to Montana employers on combined wage claims is an equity issue. We would like to program the BeAR system to accommodate the combined wage bill back. We do not agree that the cost involved in programming this process would be regained through the resultant increase in employers' contributions.

We do not believe that the charge backs would greatly affect most employers tax rates or that there is a measurable effect on the Trust Fund by not charging back these amounts. The estimated $2,000,000 in a 1985 study referred to the total amount paid out on combined wage claims. This did not reflect the historical percentage that is not chargeable due to separation issues as identified in the 1994 study. The amount would be considerably less with this consideration.

We do not have programmer resources at this time to implement this system change. The time estimate indicates it would take one dedicated programmer at least a year to complete the required programming. We have two trained BeAR programmers at this time who are utilized to capacity maintaining the current system and implementing state and federal requirements. They are also dedicating considerable time and effort to training new staff.

We lack funding sources at this time to contract the programming to outside resources. If we are successful in obtaining additional automation funding this option is a possibility.

We will continue to evaluate the possibility of implementing combined wage charge backs in the interest of equitable treatment of employers based on available funding.

We have updated our request for programming (RFP) for this project and have added it to our outstanding list in the event monies are received.

RECOMMENDATION # 14

We recommend the department:

A. Ensure only authorized personnel have access to change employer tax rates.

AGENCY RESPONSE - Concur. In the new tax system, currently being developed, the ability to add rates to the system will be allowed on only two screens. In both instances, access to those screens will be strictly limited to persons who need access to perform their specific job duties. In addition, other procedures test the accuracy of rates input. Three Revenue Quality Control reviews are conducted annually that involve verification of accuracy of rate assignments. A sample of 60 new status determinations, 60 successor status determinations, and 60 experience rate assignment determinations are pulled and reviewed to ensure that employer tax rates are assigned according to law. These reviews have not identified a problem involving the assignment of employer tax rates.

B. Retain the rate discrepancy reports for a specified period of time.

AGENCY RESPONSE - Concur. A rate discrepancy list will be produced off the new tax computer system and will be retained for three years.